Campus Communication
DRAKE UNIVERSITY

February 7, 1984

To: Jim Cooney
From: Robert W. Lute
Subject: Damage Estimates Due to KWWL-TV Actions

This memo outlines damages suffered by Drake University as a result of the actions taken by KWWL-TV last week in which they commissioned penetration of our academic computer system. It is appropriate to remember what is implied by a penetration. When a system is penetrated, the perpetrator acquires ALL system privileges. This means that the perpetrator may examine, modify or delete any or all programs, data or procedures which are stored in the computer system and may deny any or all other users access to any or all system resources. In other words, total control of the computer system and all stored data is placed at the whim of the intruder, and the intruder's actions are only limited by the intruder's imagination and ability to manipulate the system.

It must also be recognized that the actions by KWWL-TV have served to highlight the Drake University academic computing system as a target for potential "hackers", beyond those directly involved in the current incident. They may well have initiated a cycle of testing to attack our system which might not otherwise have occurred without the legitimitizing influence of such actions.

The following lists areas of damage and assigns approximate amount of damage suffered:

1. Following notification of the intrusion, the Academic Computing system was removed from service from 1:30 p.m. until 8:30 p.m. on Wednesday, February 1, 1984. During this period, all user files which had been changed since the last full backup, were loaded to tape. Both user disks were removed from service, and the backup versions were installed. Finally, user files were reloaded. These protective measures were required to reasonably assure that the intruders had not left hidden procedures on these disks which would cause damage in the future by deleting or modifying files or otherwise damaging the computer system. Analysis of the corresponding time period on the next day indicates that the value of lost computer time during this shutdown is approximately $3,250. The value of the user's time during this period when they could not access the system is valued at approximately $1,350. When the system was shut

down, the system held research jobs which were in progress. These jobs were lost and had to be restarted when the system was returned to service. The value of the lost computing is $340. Thus the total damage estimate for this item is $4,940.

2. Since the report of the incident, the cost of time devoted to this problem by Computer Center staff amounts to $1,500. This amount will continue to increase at $250 per day until this whole episode is concluded. The staff continues to search for the details of the techniques used by the penetrators, and to work with our vendor and systems personnel in other universities using similar systems to determine appropriate corrective action to take in response to this penetration. These estimates do not take into account the time spent by senior administrative officials of the University, nor time spent by Student Life staff in preparing for and handling the disposition of disciplinary proceedings regarding Ronald Boster.

3. To minimize the possibility that the penetrators have left behind materials which will enable future penetrations or will cause damage in the future, it will be necessary to take additional steps. The steps recommended by our computer vendor will involve a cost of $2,640 to purchase a clean version of the present operating system from Digital Equipment Corporation and will take an estimated 20 clock hours of processing and staff time. Total estimated cost for these steps involving loss of access to users, computer time and staff time is $13,000.

4. It will be necessary to modify the current availability of dial-up ports on the computer system to improve their security. It was via one of these ports that the penetration occurred. These ports will be modified to enhance security, by the addition of specialized communications equipment. Initial cost estimates for this equipment are in the $30,000 to $50,000 price range. In addition, Drake users who wish to access the dial-up ports via this technique will require advanced communications devices. The per user cost is approximately $1,000. At present, it will be necessary to purchase about 60 of these units to serve existing student, faculty and staff users. Total cost of this additional protection will be in the $90,000 to $110,000 range.

5. Steps have already been taken to activate additional system monitoring functions to better enable detection of penetrations, and to aid in the

determination of how penetrations were accomplished. These steps require use of system resources which were formerly available to our user community. It is our best estimate that we are now able to serve 10% fewer users than in the past. The annual cost for this decrease in service is $45,000 in computer time and $40,000 in lost user time.

6. To analyze the results of the monitoring functions mentioned in item 4, it is necessary to activate a series of specially written computer programs. These programs will operate at non-prime time, and will impact our research users. It is estimated that processing costs for these tasks amount to $50 per day, with attendant loss of this valuable time to our research users who operate under research contracts with external agencies. Annual cost for this decrease in service is $18,250.

7. Based on the heightened awareness of the "hacker" community due to this incident, one staff member will be spending a minimum of half his time on operating the monitoring systems, taking corrective actions based on what is observed, working with the vendor to improve security measures within the operating system. Estimated annual costs for this effort are $15,000.

8. Since we will no longer be able assure our external customers of the confidentiality of the data which they store on the academic computing system, we may expect the loss of the income which they provide to support computing at Drake University. This income amounts to $22,000 per year.

As a direct result of the penetration which occurred at the hands of KWWL-TV we have suffered immediate loss of $6,440. We will suffer loss of an additional $14,000 during the next month. Installation of the additional dial-up security system will cost $90,000 to $110,000. Operating losses which continue due to the incident amount to $140,250 on an annual basis. If further penetrations occur and are detected, additional losses on the scale of the immediate losses mentioned above will also be experienced for each such incident. That is to say, the losses mentioned in this document represent a minimum estimate.